PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-089737
(43)Date of publication of application : 15.04.1991

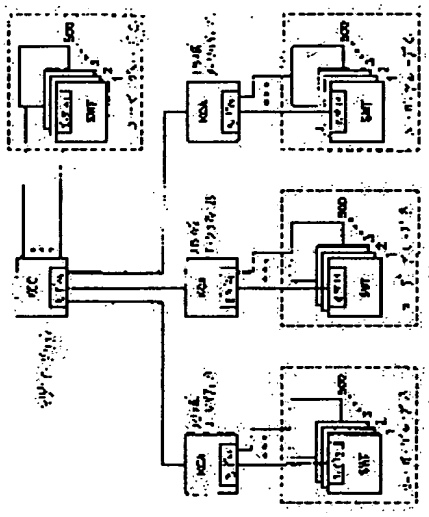
(51)Int.Cl. H04L 9/06
H04L 9/14

(21)Application number : 01-217593
(22)Date of filing : 25.08.1989

(71)Applicant : MOTOROLA INC
(72)Inventor : ROBERT IVAN FOSTER
ROBERT FREDERIC PFEIFER
THOMAS JAMES MIM JR

(54) HIERARCHICAL KEY MANAGEMENT SYSTEM

(57)Abstract:
PURPOSE: To establish secret protection between terminal users by providing the system with plural key permission authority means, corresponding to user groups and a terminal means groups and a key permission center means for applying authority to each of the key permission authority means and permitting direct secret protection communication between the terminals of different groups.
CONSTITUTION: A terminal group in the hierarchical key management system corresponds to one of user groups, and a large number of users can execute secrecy protective communication with other users by respective terminals SWT through a public exchange telephone network. The system has plural key permitting authorities(KCAs), and each KCA permits a user in a certain group to use a terminal for executing secrecy protective communication with another user in the same user group. The system has also key permission centers (KCCs), and each KCC is connected to plural KCAs to provide permission authority to each KCA and permit secret protection communication between different user groups. Consequently direct secrecy protection between terminal users can be established.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−89737

⑤Int.Cl.⁵　識別記号　庁内整理番号　⑬公開　平成3年(1991)4月15日

H 04 L 9/06
9/14

6914−5K　H 04 L 9/02　Z

審査請求　未請求　請求項の数 10　(全9頁)

⑭発明の名称　階層型キー管理システム

⑳特　願　平1−217593

㉒出　願　平1(1989)8月25日

⑫発明者　ロバート・イワン・フオスター　アメリカ合衆国アリゾナ州メサ、イースト・ヘイル・サークル4023

⑫発明者　ロバート・フレデリック・フエイファー　アメリカ合衆国アリゾナ州スコツツデイル、イースト・アコマ・ドライブ5236

⑫発明者　トーマス・ジエームス・ミム・ジユニア　アメリカ合衆国アリゾナ州メサ、イースト・フエアフイールド5926

⑪出願人　モトローラ・インコーポレーテツド　アメリカ合衆国イリノイ州シヤンバーグ、イースト・アルゴンクイン・ロード1303

⑭代理人　弁理士　本城　雅則　外1名

明　細　書

1．発明の名称

階層型キー管理システム

2．特許請求の範囲

1．複数のユーザの一部が交換回線網を経由して機密保護通信を行うことを可能にする階層型キー管理システムにおいて、前記階層型キー管理システムは：

前記ユーザの予め定めるユーザ・グループ；

共通のオーソリティによって予め許可されている前記各ユーザ；

前記交換回線網に接続され、前記交換回線網を経由して機密保護通信を行う端末手段；

端末手段のグループであって、各グループは前記ユーザのグループに対応し、第1端末手段が前記交換回線網を経由して第2端末手段と通信を行う前記端末手段のグループ：ならびに

前記第1および第2端末手段は、前記共通オーソリティに接続されることなく、前記交換回線網を経由して機密保護通信を直接行うことを特徴とする階層型キー管理システム。

2．前記共通オーソリティが：

ユーザ・グループの前記ユーザを許可する複数のキー許可オーソリティ手段であって、前記キー許可オーソリティ手段はユーザ・グループおよび端末手段グループに対応し、各キー許可オーソリティ手段は前記ユーザ・グループの他のユーザと直接機密保護通信を行うために前記端末手段を使用することを許可し、前記複数の各キー許可オーソリティ手段は前記対応するグループの前記端末手段に接続される前記複数のキー許可オーソリティ手段；および

前記複数の各キー保障オーソリティ手段に接続されたキー許可センタ手段であって、前記許可センタ手段は許可オーソリティを前記キー許可オーソリティ手段の各々に与え、異なったグループの端末手段の間で直接機密保護通信を認める前記キー許可センタ手段によって構成されることを特徴とする請求項1記載の階層型キー管理システム。

3．個々のユーザに対応し前記端末手段に接続可能な機密保護動作装置手段をさらに有し、前記機密保護動作装置手段は前記端末手段に対して転送を行うため認証、符号化および復号化情報を格納するために動作することを特徴とする請求項2記載の階層型キー管理システム。

4．前記機密保護動作装置手段は、前記端末手段にさらに接続され、前記端末手段が許可情報によって前記機密保護動作装置手段をプログラムすることを可能にすることを特徴とする請求項3記載の階層型キー管理システム。

5．前記機密保護動作装置手段は前記端末手段にさらに接続され、前記端末手段が再発生した通信情報によって前記機密保護動作装置手段を繰返して再プログラムすることを可能にすることを特徴とする請求項4記載の階層型キー管理システム。

6．前記ユーザ・グループのユーザは、サービスを行っていないユーザ・グループのキー許可認証手段の条件によって前記キー許可センタ手段に直接接続されることを特徴とする請求項2記載の階層型キー管理システム。

7．少なくとも2つの端末間で電話回線網を経由して機密保護通信を行い、前記各端末が共通のオーソリティから以前の許可を受け取る方法において、前記方法は：

前記2つの端末間で情報の転送を行うため電話回線網を経由する接続を完了する段階；

前記共通のオーソリティの符号化キーの下で前記2つの端末間で符号化キーを交換する段階；

端末に対して各々の転送およびキー対を決定し、前記2つの接続された端末間での機密保護通信を可能にする段階；および

引き続き行われる機密保護通信のため各端末に特有の第2の変更した符号化／復号化キー対を保存する段階によって構成されることを特徴とする方法。

8．機密保護動作装置を前記端末に挿入し、対応する端末の各ユーザが機密保護通信を行なえることを許可する段階をさらに有することを特徴とする請求項7記載の方法。

9．前記機密保護動作装置に含まれる情報を前記端末によって検証し、前記ユーザが現在許可されていることを保証する段階をさらに有することを特徴とする請求項8記載の方法。

10．複数のユーザが電話回線網を経由して機密保護通信を行うことを許可する階層型キー管理システムにおいて、前記階層型キー管理システムは：

前記ユーザの予め定めるユーザ・グループ；

各グループがユーザの前記グループに対応する端末手段のグループであって、前記各端末手段は前記電話回線網を経由して他のユーザとあらかじめ定めるユーザ数まで機密保護通信を行うことを可能にする前記端末手段のグループ；および

ユーザ・グループの前記ユーザが前記ユーザ・グループの他のユーザと機密保護通信を行うために前記端末手段を使用することを許可し、または異なったユーザ・グループのグループ間の機密保護通信を認めるキー許可手段によって構成されることを特徴とする階層型キー管理システム。

3．発明の詳細な説明

（産業上の利用分野）

本発明は、機密保護機能のある電気通信システムに関し、さらに詳しくは、ユーザの認可および認証を行う権限を有する代表者を支援する拡張性のある階層型キー管理システムに関する。

（従来の技術）

代表的なキー管理システムは、1986年3月25日J．エバーハート等に付与された米国特許第4,578,531号に示されている。この発明は、機密保護機能のある複数の各端末に接続されたキー分配システムを開示する。機密保護のあるデータ伝送を希望する場合、各端末はキー分配センタとの通信を確立しなくてはならない。これによりキー分配センタは、端末の資格審査を行い、必要な機密保護の分析を実行する。

（発明が解決しようとする課題）

このシステムの欠点は、キー分配センタが、全ての2つの端末間のそれぞれの機密保護通信に関与しなくてはならないことである。端末は、自己

の情報の機密保護パケットをキー分配センタを経由してのみ交換する。各端末は、検証のために許可情報をキー分配センタに送り、その結果得られる情報をキー分配センタから受信しなければならない。このような多重通信は効率的でない。

さらに、上述のシステムは、機密保護が階層的になっていない。全ての重要なキー・データがセンタに集中しているので、もしキー分配センタの機密保護が危険にさらされると、各ユーザの機密保護もまた危険にさらされる。

したがって本発明の目的は、端末ユーザ間で直接機密保護を確立することのできる階層型のキー分配システムを提供することにある。

（課題を解決するための手段）

本発明の目的を達成する場合の新規な階層型キー分配システムを示す。

階層型キー管理システムは、複数のユーザに公衆交換電話回線網を経由する機密保護通信を許可する。階層型キー管理システムは、ユーザを限定したユーザ・グループに割当てる。

階層型キー管理システムは、端末群を含む。各端末群はユーザの１つのグループに対応する。各端末によって、多数のユーザが公衆交換電話回線網を経由して他のユーザと機密保護通信を行うことが可能になる。

階層型キー管理システムは、複数のキー許可オーソリティ（key certification authority ：ＫＣＡ）を有している。このキー許可オーソリティは、ユーザ・グループのユーザが上記のユーザ・グループの他のユーザと機密保護通信を行うために端末を使用することを許可する。

階層型キー管理システムは、またキー許可センタを有している。この各キー許可センタは複数の各キー許可オーソリティに接続される。キー許可センタは許可オーソリティを各キー許可オーソリティに与え、異なったユーザ・グループ間での機密保護通信を認める手段を提供する。

（実施例）

第１図は、キー管理システムの階層を示す。キー許可センタ（key certification center：ＫＣＣ）はこのシステムの中核をなすオーソリティである。ＫＣＣは、キーボード、表示端末、ハードディスク、バックアップ用テープ・ストリーマ、プリンタおよび通信用インタフェイス端末（network interface terminal ：ＮＩＴ）を有する専用の特別の目的に供するコンピュータ・システムで構成することが可能である。ＮＩＴは、以下で説明する。

各ＫＣＡおよびＫＣＣは、公衆交換電話回線網を経由してＫＣＡおよびＫＣＣの高速度の電話による接続を行うモデムを有する。他の通信伝達手段を使用することも可能である。３つのＫＣＡは、第１図に示す地域オーソリティＡ、地域オーソリティＢ、地域オーソリティＣである。しかし、ＫＣＣに４つ以上のＫＣＡを接続することも可能である。

各ＫＣＡはまた、キーボード、表示端末、ハード・ディスク、バックアップ用テープ・ストリーマ、プリンタおよび通信用インタフェイス端末を有するコンピュータ・システムで構成される。各地域オーソリティすなわちＫＣＡは、５００以上のユーザを取り扱うことが可能であるが、一般的に最高５００のユーザ間で機密保護通信を提供する。例えば、地域オーソリティＡは、ユーザ・グループＡのユーザ間で機密保護通信を可能にする。各ユーザのグループＡ、Ｂ、およびＣは、典型的には最高５００の機密保護線路端末（secure wireline terminal：ＳＷＴ）によって構成される。ユーザとは、ユーザ・グループ内で１つ以上のＳＷＴを使用することを許可された個人である。

各ＳＷＴは、トラフィック・キーの機密保護交換用の非対称キーを発生する。ＳＷＴは、端末のアクセスおよびユーザ保障用の機密保護作動装置（security activation device：ＳＡＤ）を有する。このＳＡＤは、最初にＫＣＡによってプログラムされ、続いてＳＷＴによって再プログラムされる物理的なキーである。このＳＡＤは、機密保護通信およびユーザの認定を可能にするためにＳＷＴのコンセントに挿入される。

このＳＷＴは、各ユーザ用の独特で非対称な一

対の符号化／復号化キーを発生する。この非対称な一対のキーは、地域オーソリティ（ＫＣＡ）によって許可される。２つ以上のＫＣＡを有する大きな通信システムの場合、あるユーザ・グループに属するユーザは、他のユーザ・グループのユーザとの通話を希望する可能性がある。この場合、グループ間で通話を行うユーザは、共通するＫＣＣに登録されたＫＣＡによって許可されなくてはならない。

もしユーザの地域オーソリティ（ＫＣＡ）が一時的にサービスを行っていない場合、ＫＣＣはサービスを行っていない全てのＫＣＡをバックアップすることができる。これは、サービスを行っていないＫＣＡのバックアップ・テープをＫＣＣにロードすることによって行われる。

最初に、機密保護通信のユーザは、その地域オーソリティ（ＫＣＡ）によってシードＳＡＤ(seed ＳＡＤ)、および対応するパスワードが発行される。このシードＳＡＤは、第１すなわち最初のＳＡＤであることから自分の名前を得、そのＳＡＤから個々のユーザに関する機密保護情報が発生される。このシードＳＡＤは、ユーザの識別に関するデータおよび許可に必要な特別コードを有する。

ユーザは、ＳＷＴに自分のＳＡＤを挿入することによって許可を受けることが可能である。次に、ユーザは自分の地域オーソリティであるＫＣＡに通話を試みる場合、パスワードを入力する。このＳＡＤおよびパスワードを使用して、ユーザは最大８つのＳＷＴで許可を受けることが可能である。さらに、最高８名のユーザが個々のＳＷＴで許可を受けることが可能である。ＳＷＴ１台当たりのユーザ数およびユーザ１名当たりのＳＷＴ数は典型的には８に設定されるが、ＳＷＴ１台当たりのユーザ数およびユーザ１名当たりのＳＷＴ数をより多くする柔軟性が与えられている。

ユーザが一度特定のＳＷＴで許可されると、このユーザは、同じ地域オーソリティ内の他のユーザと、または自動化されたキー発信および２つの端末を連結して行われる分配プロセスを介して、共通のＫＣＣを共有する他のユーザと機密保護通話をすることが可能である。すなわち、ユーザ・グループＡに属するユーザは同グループに属する他のユーザと通話が可能であり、またはグループＢに属するユーザ、またはグループＣに属するユーザと通話可能でありまたその逆も可能である。ＳＷＴのユーザが一度許可を受けると、このユーザは、公衆交換電話回線網（public switched telephone network ：ＰＳＴＮ）または他の回線を介して通常の通話が可能である。この通話が機密保護通話であるべきであると決定されると、ＳＷＴ上の機密保護押しボタンが押される。特定の通話における２つのＳＷＴは許可データを交換し、トラフィック・キーを発生しこれを交換する。この時点で機密保護通信が確立する。この同期および機密保護プロセスの一部として、他のパーティの識別および接続の機密保護レベルのような認証情報がＳＷＴ上に表示される。

ユーザの許可の時点で、ＫＣＡは終期コードを許可されているユーザのＳＡＤまたはキーに付加する。このユーザのＳＡＤの終期に先立ち、このユーザは自分のＳＡＤを再許可するように告知される。再許可のためには、ユーザは自分のパスワードおよびＳＡＤを使用して地域ＫＣＡを呼ぶ。再許可の間、端末はＫＣＡによって許可される新規の非対称符号化／復号化キーの一対とユーザのＳＡＤに付加され、格納される新しい終期を発生する。もしユーザが終期日に先立ってＫＣＡによる再許可を行なわなかった場合、ＳＷＴはこのユーザのシステムへのアクセスを自動的に拒絶する。

オーソリティはこのキー管理システム全体を委任されている。ＫＣＣおよびＫＣＡは各ユーザまたはＳＷＴの個人用キーを持たない。従って、もしＫＣＡまたはＫＣＣのいずれか１つが危険にさらされる場合でも、キー管理システム内の全てのユーザが危険にさらされることはない。しかし、ＫＣＣまたはＫＣＡが危険にさらされていると、誤った許可を与える可能性がある。

オーソリティの代表権は、ＫＣＡがＫＣＣにオーソリティとして登録されるプロセスを通して確

立される。このことは、ＰＳＴＮによる機密保護プロセスを使用して行われる。一度ＫＣＡがＫＣＣに登録されると、ＫＣＡは個々のユーザの許可プロセスの一部として登録パケットを発行することができる。これらの登録パケットによって、ユーザは他の地域オーソリティ・グループ（ユーザ・グループＡ、ＢまたはＣ）のユーザと機密的に通信をすることができる。

ＫＣＡは、新規の非対称通信領域キーを許可し、総括的な承認されてないキー情報を受信するため、規則的な間隔でＫＣＣに対して再許可プロセスを実行する必要がある。ＫＣＡとＫＣＣとの間で発生するこの処理は、メッセージの内容を除き、ＳＷＴとＫＣＡとの間で行われる許可処理と同様である。

ＫＣＣは、総括的な承認されていないキーの一覧（unauthorized key list ：ＵＫＬ）を保持し分配する。このＵＫＬの分配は、システムの階層を介して行われる。ＫＣＡは、これらの各ＳＷＴユーザからＵＫＬを受信する。ロックアウト・パケット（Lockout packet）であるこのデータはＫＣＣに送信され、グローバルＵＫＬを更新する。このグローバルＵＫＬは、次にＫＣＡを介して各ＳＷＴに分配される。ＵＫＬ上でのユーザに対する機密保護期間はＳＷＴによって自動的に防止される。もしこの構成にＫＣＣが設けられていない場合、ＵＫＬはＫＣＡ中に格納される。

ＫＣＡによってシードＳＡＤが作られた時点からＫＣＡがゼロになる（クリアされるかリセットされる）迄、すなわち無くなるか満了する迄、キー管理システムは該当するＳＡＤの使用を監視し、修正しかつこれに対する責任を負う。ＫＣＡによって一度ユーザが許可されると、２つのＳＷＴ間に機密保護通信伝送路を確立するために端末から端末間のみの通信が必要となる。これらの通信によって、ＳＷＴ間に機密保護チャンネルが確立される。ユーザが自分のＳＷＴの機密保護押しボタンを押した場合、一連のメッセージがＳＷＴ間で交換される。この交換される情報の幾つかは、ＳＷＴのモデムのチャンネル特性を示す。

第２図は、ＳＷＴのユーザ１ＡとＳＷＴのユーザ５Ａとの間の機密保護通話を示す。ＳＷＴのユーザ１Ａと５Ａは、同一の承認を行うオーソリイティ、すなわち、第２図に示すＫＣＡ　Ａによって許可されるものとして示される。以下の説明は、ＳＷＴ　１Ａと５ＡがそれらのＳＡＤ（機密保護実行装置）キーを以前に許可している仮定している。このことは、ＳＷＴ　１Ａおよび５ＡをＫＣＡ　Ａに接続する線によって示され、かつ許可されたＳＡＤキーによって示される。それ以前の時点で、ＳＷＴ　１Ａと５Ａは、いずれもこの許可プロセスを実行している。

ＳＷＴ　１Ａおよび５Ａは電話回線を介して予め接続を確立している。この時点で、ユーザはＳＴＷ　１Ａの機密保護押しボタンを押す。これによって、ＰＳＴＮを経由して自動メッセージ交換が開始され、その結果、ＳＷＴ　１Ａと５Ａとの間に機密保護のされた２４００ボーの伝送路が確立される。２４００ボーの伝送路は１例である。確立されたデータ伝送路は、いずれのデータ・レートであってもＳＷＴによって実行される。

次の第１表は、以下で使用する種々の符号化および復号化ベクトルの略語リストである。

第１表

Ｅｘ	－	ユーザの符号化ベクトル
Ｄｘ	－	ユーザの復号化ベクトル
Ｅｘａ	－	キーのオーソリティ符号化ベクトル
Ｄｘａ	－	キーのオーソリティ復号化ベクトル
Ｅａｘ	－	キーのオーソリティ許可符号化ベクトル
Ｄａｘ	－	キーのオーソリティ許可復号化ベクトル
Ｅｃ	－	キーの許可符号化ベクトル
Ｄｃ	－	キーの許可復号化ベクトル
Ｅｘｔｓ	－	ユーザの許可符号化ベクトル
Ｄｘｔｓ	－	ユーザの許可復号化ベクトル

各ユーザは、自分の許可されたＳＡＤキーをそ

れぞれのＳＷＴに挿入する。最初に、２つのＳＷＴはアクセス／領域メッセージを交換する。これらのメッセージは、１つのオーソリティＩＤ（ＫＣＡの識別）、バージョン番号、Ｄａｘ用終期データ、中央ＩＤ（ＫＣＣの識別）、バージョン番号、Ｄｃ用終期データ、端末のタイプおよび端末のシリアル番号を有する。両ＳＷＴは送信されたメッセージを検査し、共通の非対称通信領域キー、ＤａｘまたはＤｃのいずれかと一致させようとする。両ＳＡＤがＫＣＡによって許可されるので、一致が起こる。

次に、各ＳＷＴは他方に認証パケット・メッセージ（Authentication Packet message ）を送る。この認証パケット・メッセージには以下の情報が入っている。すなわち、これらは、ユーザのＩＤサイン（ＩＤ signature：ＩＤＳ）、ユーザのＩＤ、ＳＡＤのシリアル番号（ＳＡＤ serial number ：ＳＳＮ）、アクセス情報、端末のシリアル番号（Terminal serial number：ＴＳＮ）、およびユーザの許可された非対称キーＥｘｔであるＫｇのキーイングに使用される。ＲＣのコピーの１つが地域送信Ｋｇに転送される。ＲＣの他のコピーは他方のユーザＥｘｔを用いて符号化される。各ＳＷＴは、この時点でランダム成分メッセージ・パケットを他方のユーザに送信し、これは他方のユーザＥｘで符号化される。各ＳＷＴが他方のランダム成分メッセージ・パケットを受信すると、Ｄｘｔを用いてそのパケットを復号化する。ランダム成分は受信Ｋｇのキーであり、またキーをかけるのに使用されてきた。

最後に、クリプト同期（Crypto Sync ：ＣＳ）メッセージ・パケットが各ＳＷＴによって発生される。ＳＷＴ　１Ａおよび５Ａは、次にＰＳＴＮを経由してクリプト同期（ＣＳ）メッセージ・パケットを交換する。各ＳＷＴは、次に他のＳＷＴから受信したクリプト同期メッセージを処理する。クリプト同期メッセージは受信Ｋｇによって処理され、クリプト同期を得る。クリプト同期が達成されると、各ＳＷＴは自分のユーザに、機密保護伝送路が適切なボー・レートで確立されたことを知らせる。

もし２つのＳＷＴ間の通信が２４００ボー・レートで行われる場合、上記の機密保護処理は約１０秒を要する。誤りの影響を最小にするため、データ交換に対して順方向エラー修正（forward error correction ）が使用される。

第３図では、ＳＷＴユーザ１ＡからＳＷＴユーザ７Ｂへの機密保護通話を説明する。ＳＷＴユーザ１ＡはＫＣＡ　Ａによって許可されている。ＳＷＴユーザ７Ｂは、あらかじめＫＣＡ　Ｂによって許可されている。これは、ＳＷＴ　１ＡとＫＣＡ　Ａとの間およびＳＷＴ　７ＢとＫＣＡ　Ｂとの間の破線によってそれぞれ示される。ＫＣＡ　ＡおよびＫＣＡ　Ｂはキー許可センタ（ＫＣＣ）Ｘによって予め許可されている。前述のように、ＳＷＴ　１ＡおよびＳＷＴ　７Ｂは非機密保護の状態でＰＳＴＮを介して相互に接続される。ＳＷＴ　１Ａのユーザは、機密保護押しボタンを押し、その結果、アクセス／領域メッセージ・パケットがＳＷＴ　１Ａと７Ｂと間に送信される。これらのアクセス／領域メッセージはＫＣＣ　ＩＤおよびバージョンを有しているので、アクセス／領域メッセージ・パケットは一致する。異なったＫＣＣに属するＳＷＴ間の機密保護通話は、このシステムの下では認められていない。

ＫＣＡではなくＫＣＣの同一性によって一致が判定されるので、ＳＷＴ間の次のメッセージ送信は、上述の共通なＫＣＡの場合とは異なったものになる。この場合のＳＷＴ間の次のメッセージ・

パケットの送信は登録パケット（Registration Packet）と呼ばれる。この登録パケットは以下の情報で構成される。すなわちこれらは、承認を行うＫＣＡの非対象領域キー（Ｄａｘ）、ＫＣＡのＩＤおよび各ＫＣＡに関するアクセス情報である。登録パケット全体はＫＣＣの領域キーＥｃを使用して復号化される。各ＳＷＴは他の登録パケットを受信し、共通の領域キーＤｃを用いて復号化する。結果として、各ＳＷＴは他方の非対象領域キーＤａｘを抽出する。各ＳＷＴが他方のＫＣＣの同一性およびバージョンが正しく一致すると判定した場合、上述のように機密保護プロセスが行われる。もしＫＣＣのＩＤおよびバージョンが一致しない場合、機密保護通話は終了する。

登録パケット・メッセージが正しく復号化された後、認証メッセージ・パケットがＳＷＴ　１Ａと７Ｂとの間で交換される。認証パケット・メッセージに対する処理が、共通のＫＣＡの場合に対して、上述したように行われる。次に、ランダム成分メッセージ・パケットがＳＷＴ　１Ａと７Ｂとの間で交換される。再び、この処理も上述のように共通のＫＣＡに対して行われる。最後に、クリプト同期メッセージ・パケットがＳＷＴ　１Ａと７Ｂとの間で交換され、上述のように処理される。

異なったＫＣＡ領域であるが、共通のＫＣＣ領域にあるＳＷＴ間での機密保護通話を行う場合、通信レートを２４００ボーと仮定すると、２つのＳＷＴ間での機密保護通話を確立するのに要する時間は約１５秒である。

第１図に示すように、ＫＣＡがサービスを行っていない場合、該当するＫＣＡを許可しているＫＣＣは、ＫＣＡのバックアップとして動作可能である。ユーザ・グループ・バックアップは、ユーザ・グループＡ、ＢおよびＣのようないずれのユーザ・グループにも提供される。これを行うため、サービスを行っていないＫＣＡのバックアップ・テープがＫＣＣにロードされる。このような構成でユーザを許可するため、ＫＣＣはＫＣＡとして動作する。

ＫＣＡに対する最初の許可は、ＳＷＴ上のＳＡＤに対するＫＣＡの最初の許可と同じ方法で行われる。ＫＣＡに対する最初の許可のため、この特定のＫＣＡに対してパスワードおよびシードＳＡＤを使用して機密保護伝送路が作られる。例えば、ＫＣＡ　Ａまたは地域オーソリティＡは中央オーソリティＫＣＣに機密保護伝送路を確立する。機密保護伝送路が確立されると、ＫＣＡは許可情報パケットを送る。このパケットは、オーソリティの識別サイン（ＩＤＳ）、端末のシリアル番号（ＴＳＮ）、Ｅｘａ、ＤａｘおよびＳＡＤのシリアル番号（ＳＳＮ）を含む。

ＫＣＣは、ユーザを許可する場合にＫＣＡがＫＣＣのために動作することを保障する登録パケットを使用してＫＣＡに応答する。さらに、ＫＣＣはＫＣＡにロックアウト・パケットを送るが、これは認定されてないキーの一覧およびグローバルな復号化キーＤｃである。登録パケットは新規に発生した非対称領域キーを有し、これらはＫＣＣのＥｃを使用して符号化される。この登録パケットはまたＫＣＡの識別およびアクセス／クリアランス情報を有する。

特定のＫＣＡ非対称領域キーの認証期間が終了した場合、ＫＣＡは新規のキーをＫＣＣで再許可する。再許可のプロセスは、あらかじめ設定された許可期間がまだ終了していないならば、グローバルな非対称領域キーＤｃがＫＣＣによって送られない点を除き、本質的に最初の許可プロセスと同様である。

ＫＣＡによるユーザの許可後、このユーザを許可した特定のＳＷＴはＳＡＤをカバーする成分を発生し、これはランダムに発生され、ＳＡＤをカバーする成分によって符号化またはカバーされるアクセス領域メッセージをＳＷＴの不揮発性メモリに記憶する。次に、このＳＷＴは認証パケット、登録パケット、ＴＳＮ（端末のシリアル番号）およびＳＡＤのカバー成分を格納する。このＳＷＴはまた認定されていないキーの一覧（ＵＫＬ）、および同じＳＡＤカバー成分でカバーされる復号化ベクトルＤｃおよびＤｘｔを格納する。使用毎

に、ＳＡＤカバー成分は更新される。

第４図は、ＫＣＣまたはＫＣＡのブロック図を示す。各ＫＣＡおよびＫＣＣはコンピュータ制御のシステムによって構成することが可能である。このコンピュータ制御システムはＣＰＵ、ハードディスク、バックアップ・テープ装置、プリンタ、キーボード、表示装置、および通信用インターフェイス端末（ＮＩＴ）によって構成される。このＮＩＴは、ＫＣＣまたはＫＣＡにインターフェイスするための特別の機密保護線路端末である。このＮＩＴは、ＫＣＡの場合ユーザのモデムの全てに接続され、ＫＣＣの場合ＫＣＡに接続されるモデムを有する。

第４図に示す制御コンソールは、表示装置、キーボード、ＣＰＵ、ハード・ディスク、バックアップ・テープ装置によって構成される。

ＮＩＴは、ユーザとＫＣＡとの間、またはＫＣＡとＫＣＣとの間でデータを高速転送する。ＮＩＴはまた、ユーザとバックアップ・モードにおいてＫＣＡとして動作するＫＣＣとの間で高速通信を直接行う。

各ＮＩＴおよびＳＷＴはモデムを有する。これらのモデムは、２４００ないし９６００ボーのような高速でデータを送る能力を有するが、これらの速度に制限されるものではない。

キーボードはＣＰＵに対してデータ入力を行う。表示装置はＣＰＵからの映像出力を行う。プリンタはＣＰＵ出力のハード・コピーによる映像表示を行う。ディスクは、ＳＷＴに関連する全てのオペレーティング・ソフトウェアおよびデータ・ベースを格納し、ＫＣＣの場合は、ＫＣＡに関する情報を格納する。バックアップ・テープ装置はサービスを行っていないＫＣＣにＫＣＡ情報をロードし、その結果、ＫＣＣはＫＣＡの機能を果たすことができる。さらに、バックアップ・テープ装置は、ＫＣＡまたはＫＣＣがサービスを行っていない場合、システムを再ロードする。

本発明の好適な実施例が図示され、この実施例が詳細に述べられたが、本発明の精神または添付の請求項の範囲から逸脱することなく、種々の変形が行われることは、当業者にとって容易であることは明らかである。

４．図面の簡単な説明

第１図は、本発明の動作原理を実現するキー分配システムを示すブロック図である。

第２図は、同じ許可オーソリティによって提供される２つの機密保護線路端末間で機密保護通話を行うブロック図である。

第３図は、異なった許可オーソリティによって提供されるが同じキー許可センタである２つの機密保護線路端末間で機密保護通話を行うブロック図である。

第４図は、キー許可センタとキー許可オーソリティのブロック図である。

ＫＣＣ・・・キー許可センタ、ＫＣＡ・・・キー許可オーソリティ、ＳＷＴ・・・機密保護線路端末、ＳＡＤ・・・機密保護作動装置、ＰＳＴＮ・・・公衆交換電話回線網

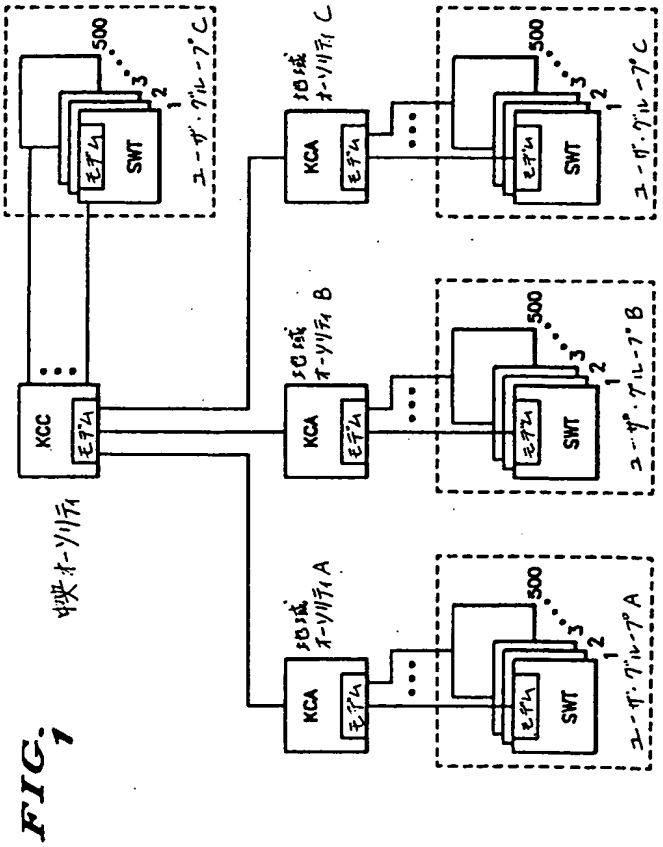


FIG. 1

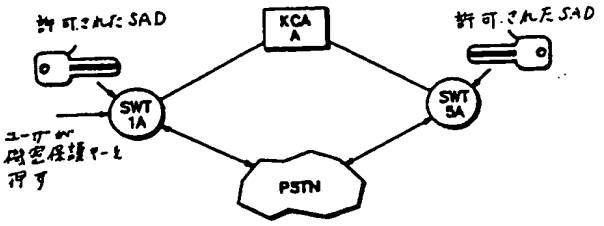
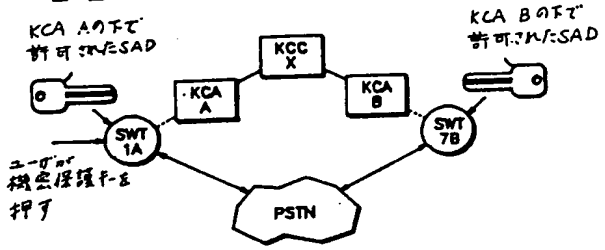


FIG. 2

FIG. 3



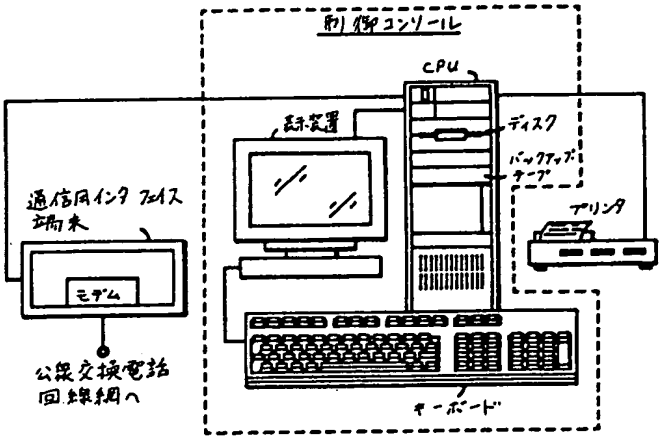


FIG. 4